Document made available under the Patent Cooperation Treaty (PCT)

International application number: PCT/KR2005/000345

International filing date: 04 February 2005 (04.02.2005)

Document type: Certified copy of priority document

Document details: Country/Office: KR
Number: 10-2004-0012380
Filing date: 24 February 2004 (24.02.2004)

Date of receipt at the International Bureau: 16 January 2007 (16.01.2007)

Remark: Priority document submitted or transmitted to the International Bureau in compliance with Rule 17.1(a) or (b)

별첨 사본은 아래 출원의 원본과 동일함을 증명함.

This is to certify that the following application annexed hereto is a true copy from the records of the Korean Intellectual Property Office

출 원 번 호 : 10-2004-0012380
Application Number

출 원 일 자 : 2004년 02월 24일
Date of Application FEB 24, 2004

출 원 인 : 소프트캠프(주)
Applicant(s) SoftCamp

2007 년 01 월 15 일

특 허 청
COMMISSIONER

【서지사항】

【서류명】 특허출원서

【권리구분】 특허

【수신처】 특허청장

【참조번호】 0273

【제출일자】 2004.02.24

【발명의 국문명칭】 가상 디스크를 이용한 응용 프로그램 별 접근 통제시스템과 그 통제방법

【발명의 영문명칭】 Control system for access classified by application in virtual disk and Controling method thereof

【출원인】

【명칭】 소프트캠프(주)

【출원인코드】 1-1999-041351-3

【대리인】

【성명】 박천도

【대리인코드】 9-2000-000134-4

【포괄위임등록번호】 2004-012044-0

【대리인】

【성명】 이상문

【대리인코드】 9-2000-000136-7

【포괄위임등록번호】 2004-012045-7

【발명자】

【성명의 국문표기】 배환국

【성명의 영문표기】 BAE,Steve

【주민등록번호】 710103-1560018

【우편번호】 151-805

【주소】 서울특별시 관악구 봉천2동 41-30

【국적】 KR

【발명자】

【성명의 국문표기】 김도균

【성명의 영문표기】 KIM,Do Gyun

【주민등록번호】 681010-1249115

【우편번호】 476-833

【주소】 경기도 양평군 옥천면 용천리 188-1

【국적】 KR

【발명자】

【성명의 국문표기】 강홍석

【성명의 영문표기】 KANG,Aiden

【주민등록번호】 770113-1927716

【우편번호】 138-837

【주소】 서울특별시 송파구 삼전동 11-3 101호

【국적】 KR

【발명자】

【성명의 국문표기】 이희국

【성명의 영문표기】 LEE,Hee Gook

【주민등록번호】 761024-1452717

【우편번호】 422-826

【주소】 경기도 부천시 소사구 괴안동 157-5 보강빌라 201호

【국적】 KR

【심사청구】 청구

【취지】 특허법 제42조의 규정에 의한 출원, 특허법 제60조의 규정에 의한 출원심사 를 청구합니다.

대리인 박천도 (인)

대리인 이상문 (인)

【수수료】

【기본출원료】	39	면	38,000 원
【가산출원료】	0	면	0 원
【우선권주장료】	0	건	0 원
【심사청구료】	5	항	269,000 원
【합계】	307,000 원		

【요약서】

【요약】

본 발명은 로컬 네트워크(LAN) 또는 공용 PC 상에서 통합관리되는 데이터(프로그램 소스 또는 설계도 등이 담긴 파일)가 내부 인가자에 의해 유출되는 것을 방지하는 한편, 외부인의 접근은 차단되도록 된 접근 통제시스템에 관한 것으로, 하드디스크의 일정공간을 파일형식으로 점유하는 VSD이미지파일모듈과; 상기 VSD이미지파일모듈 내의 보안파일을 처리하는 VSD드라이브와; 상기 VSD이미지파일모듈과 VSD드라이브 간의 데이터 입출력을 암복호화 처리하는 암복호화모듈과; 상기 VSD드라이브를 통해 운영체제가 별도의 디스크볼륨이 생성된 것으로 인식시켜 상기 VSD이미지파일모듈 내 보안파일로의 접근을 처리하는 VSD파일시스템 모듈과; 상기 어플리케이션 모듈에 의한 상기 디스크드라이브 및 VSD드라이브 내 파일로의 접근시, 해당 작업이 진행되는 공간이 상기 디스크드라이브인가 VSD드라이브인가를 확인하고, 해당 파일로의 접근허가에 대한 어플리케이션 모듈의 인가여부를 판별하여 접근을 결정하는 접근통제장치;가 포함된 것 것이다.

【대표도】

도 2

【명세서】

【발명의 명칭】

가상 디스크를 이용한 응용 프로그램 별 접근 통제시스템과 그 통제방법 {Control system for access classified by application in virtual disk and Controling method thereof}

【도면의 간단한 설명】

<1> 도 1은 본 발명에 따른 접근 통제시스템의 구동관계를 도시한 블럭도,

<2> 도 2는 본 발명에 따른 접근 통제시스템의 구성에 대한 일실시예를 도시한 블럭도,

<3> 도 3은 본 발명에 따른 접근 통제시스템의 가상 디스크 설정과정을 도시한 블럭도,

<4> 도 4a는 종래 시스템 서비스 테이블의 구동관계를 도시한 블럭도,

<5> 도 4b는 본 발명에 따른 접근 통제시스템에서 적용되는 시스템 서비스 테이블의 구동관계를 도시한 블럭도,

<6> 도 5는 도 4b의 구성에 따라 응용 프로그램(어플리케이션 모듈)에 의한 해당 파일의 접근 허가여부가 진행되는 플로우를 도시한 예제,

<7> 도 6a는 본 발명에 따른 접근 통제시스템에서 응용 프로그램을 통한 해당 파일의 읽기과정을 도시한 플로우차트,

<8> 도 6b는 본 발명에 따른 접근 통제시스템에서 응용 프로그램을 통한 해당 파

일의 쓰기과정을 도시한 플로우차트,

<9> 도 7a는 본 발명에 따른 접근 통제시스템의 인스톨 이전 상태를 보이는 '내 컴퓨터' 창,

<10> 도 7b는 본 발명에 따른 접근 통제시스템의 인스톨 이후 상태를 보이는 '내 컴퓨터' 창.

<11> 도 8은 본 발명에 따른 접근 통제시스템의 가상 디스크가 파일로 인식되어지는 모습을 보이는 창,

<12> 도 9은 비인가된 어플리케이션 모듈을 통한 가상 디스크로의 접근시 그 시도가 거부됨을 보이는 창이다.

【발명의 상세한 설명】

【발명의 목적】

【발명이 속하는 기술분야 및 그 분야의 종래기술】

<13> 본 발명은 로컬 네트워크(LAN) 또는 공용 PC 상에서 통합관리되는 데이터(프로그램 소스 또는 설계도 등이 담긴 파일)가 내부 인가자에 의해 유출되는 것을 방지하는 한편, 외부인의 접근은 차단되도록 된 접근 통제시스템에 관한 것이다.

<14> 기업 또는 공공기관 등은 외부로부터의 비인가된 접속을 통한 불법적인 정보유출을 차단하고 내부의 중요한 기밀과 정보를 보호하기 위하여 외부망과의 접속시 일정 요건을 갖추지 않은 사람의 접근을 막거나 데이터의 침입을 사전에 방지하기 위한 방화벽등을 설치하고 있다. 이러한 방화벽은 단순히 네트워크를 통한 외부침

입을 차단하거나 외부 침입에 의해 방화벽이 해킹되면 침입사실을 탐지해 이에 대응하기 위한 솔루션으로서, 각종 해킹 수법을 이미 자체적으로 내장하여 침입행동을 실시간으로 감지/제어할 수 있는 IDS(Intrusion Delection System, 침입탐지시스템)와 같은 수동적인 방어개념의 방화벽과, IDS와는 달리 지능적인 기능과 적극적으로 자동 대처하는 능동적인 기능이 합쳐진 개념으로서 공격 시그니처를 찾아내 네트워크에 연결된 기기에서 수상한 활동이 이뤄지는지를 감시하며 자동으로 모종의 조취를 취하여 중단시키는 IPS(Intrusion Prevention System)와 같은 공격적인 개념의 방화벽등이 있다. 하지만, 이러한 방화벽은 로컬 네트워크(LAN) 또는 PC로의 외부 침입자에 대한 응용일 뿐 내부 인가자가 정보를 유출하고자 하는 경우에는 막을 수 있는 방법은 아니었다.

<15> 따라서, 내부 인가자로부터 기업 또는 공공기관 내 중요한 정보의 공개를 차단하고 불법적인 유출을 막기 위해 상기 방화벽과는 다른 개념의 보안 시스템이 요구되었다.

<16> 이에, 종래에는 OS부팅과정 전의 바이오스(BIOS)에서 수행되는 패스워드 인증을 이용하여 해당 PC의 사용권한이 있는 자만이 패스워드 입력을 통해 부팅과정을 계속 진행시켜 이를 사용할 수 있도록 하거나, 로컬 네트워크(LAN)를 통한 메인 서버로의 접근 시, 해당 DB에서는 보안이 요구되는 데이터만을 별도로 묶어 관리하면서 상기 DB로의 접근을 요청하는 클라이언트 PC가 상기 DB로의 접근이 인가된 것인가를 확인하여 접속여부를 결정하도록 하였다.

<17> 이외에도, 지문인식 및 홍채인식과 같은 별도의 생체인식장치를 통해 정당사

용권자만이 보안이 요구되는 데이터가 저장된 DB에 접근할 수 있도록 하거나, PC 등을 사용할 수 있도록 하였다.

<18> 하지만, 내부 인가자에 대한 상술된 종래 기술은 사용이 허가된 인가자 스스로가 보안이 요구되는 데이터유출을 목적으로 하여 해당 DB 및 PC등을 사용할 수도 있으므로, 이들에 대한 데이터유출에 있어서는 무방비 상태로 남아있는 것이 현실이다. 또한, 기술의 복잡화, 세분화, 및 전문화가 진행되면서, 하나의 기술에 관련된 다수의 인가자에 의한 해당 데이터로의 접근 및 편집이 요구되므로, 근래에는 관련 데이터가 저장된 DB로의 접근에 제한을 두지않고 모든 내부 인가자가 상기 DB로 접근할 수 있도록 되거나, 보안이 요구되는 데이터와 그렇지 않은 데이터가 하나의 DB에 통합/관리되도록 하고 있다.

<19> 따라서, 내부 인가자에 의한 데이터유출을 방지하는 기술들의 요구와 더불어, 상기 생체인식장치와 같은 별도의 고가장비 추가 또는 패스워드입력 및 사용자인증과 같은 번거로운 확인절차 없이도 DB 또는 하드디스크에 통합관리되고 있는 데이터의 접근 및 편집과정이 간편하게 이루어질 수 있는 통제시스템과 통제방법이 필요시 되었다.

<20> 한편, 종래에는 기존 문서보안의 암호화 혹은 사용권한 부여의 경우 파일의 확장명에 의존하여 CAD나 프로그램 컴파일러처럼 여러 확장자와 임시파일을 생성하는 프로그램의 경우 해당 파일에 대한 암호화나 사용권한을 부여하기가 어렵다는 단점이 있다.

【발명이 이루고자 하는 기술적 과제】

<21> 이에 본 발명은 상기와 같은 문제를 해소하기 위해 안출된 것으로, 로컬 네트워크(LAN) 차원에서 하나의 DB를 통해 보안이 요구되는 데이터와 그렇지 않은 데이터가 통합관리되거나, 일반 PC 차원에서 하드디스크에 대한 물리적인 초기분할 없이 하나의 하드디스크를 통해 통합관리되는 데이터들 중, 상기 보안이 요구되는 데이터에 대한 접근 및 편집이 내부 인가자에게 요구하는 별도의 암호입력 또는 인증확인절차 없이도 자유롭게 이루어질 수 있고, 외부 침입자에 의한 해당 데이터의 유출 봉쇄는 물론, 내부 인가자를 통한 데이터 유출 또한 차단하여, 데이터로의 접근 및 이를 이용한 작업에는 지장을 주지 않으면서도 내부자에 의한 유출은 방지되는 가상 디스크를 이용한 응용 프로그램 별 접근 통제시스템과 그 통제방법을 제공함에 목적이 있다.

<22> 또한, 상술된 목적과 더불어 보안이 요구되는 파일을 개별적으로 암호화 또는 사용권한을 부여할 필요가 없는 접근 통제시스템과 그 통제방법을 제공함에 또 다른 목적이 있다.

【발명의 구성】

<23> 상기의 목적을 달성하기 위한 본 발명은,

<24> 하드디스크의 일정공간을 파일형식으로 점유하는 VSD이미지파일모듈과;

<25> 상기 VSD이미지파일모듈 내의 보안파일을 처리하는 VSD드라이브와;

<26> 상기 VSD이미지파일모듈과 VSD드라이브 간의 데이터 입출력을 암복호화 처리

하는 암복호화모듈과;

<27> 상기 VSD드라이브를 통해 운영체제가 별도의 디스크볼륨이 생성된 것으로 인식시켜 상기 VSD이미지파일모듈 내 보안파일로의 접근을 처리하는 VSD파일시스템 모듈과;

<28> 상기 어플리케이션 모듈에 의한 상기 디스크드라이브 및 VSD드라이브 내 파일로의 접근 시, 해당 작업이 진행되는 공간이 상기 디스크드라이브인가 VSD드라이브인가를 확인하고, 해당 파일로의 접근허가에 대한 어플리케이션 모듈의 인가여부를 판별하여 접근을 결정하는 접근통제장치;

<29> 가 포함된 것으로, 상기 접근통제장치는

<30> 디스크립터에 의해 포인팅되어 해당 함수의 연산이 진행되도록 하는 확장된 시스템 서비스 테이블과; 상기 어플리케이션 모듈이 상기 시스템 서비스 테이블에 요청한 함수를 연산되지 못하도록 변경한 후, 해당 작업이 진행되는 공간이 상기 디스크드라이브인가 VSD드라이브인가를 확인하고 해당 파일로의 접근허가에 대한 어플리케이션 모듈의 인가여부를 판별하여, 그 결과에 따라 상기 확장된 시스템 서비스 테이블로 변경이전의 상기 함수를 제공하거나 그 함수의 연산중지를 선택적으로 결정하는 확장된 서비스 테이블이 포함된 것이다.

<31> 또한, 하드디스크와, 디스크드라이브와, 파일시스템 모듈과, 어플리케이션 모듈과, VSD이미지파일모듈과, VSD드라이브와, 암복호화모듈과, VSD파일시스템 모듈과, 확장된 시스템 서비스 테이블과 확장된 서비스 테이블을 포함하는 접근통제장치로 된 접근 통제시스템을 통하여,

<32> (a) 상기 어플리케이션 모듈이 선택적으로 인가되는 단계;

<33> (b) 상기 어플리케이션 모듈에 의한 해당 파일로의 접근을 위해 운영체제로 함수가 호출되는 단계;

<34> (c) 상기 운영체제에 의해 상기 함수가 상기 확장된 서비스 테이블로 제공되는 단계;

<35> (d) 상기 확장된 서비스 테이블에서 상기 함수의 연산이 중지되도록 임의로 지정된 함수로 변경되는 단계;

<36> (e) 상기 확장된 서비스 테이블에서 어플리케이션 모듈에 의한 상기 파일로의 접근공간이 상기 디스크드라이브인지 VSD드라이브인지가 확인되는 단계;

<37> (f) 상기 (e)단계에서 디스크드라이브로 확인될 경우, 변경된 상기 함수가 연산이 가능하도록 복귀되어 상기 확장된 시스템 서비스 테이블로 제공되는 단계;

<38> (g) 상기 (e)단계에서 VSD드라이브로 확인될 경우, 상기 어플리케이션 모듈의 접근이 인가된 것인가가 확인되는 단계;

<39> (h) 상기 (g)단계에서 상기 어플리케이션 모듈이 인가된 것으로 확인될 경우, 변경된 상기 함수가 연산이 가능하도록 복귀되어 상기 확장된 시스템 서비스 테이블로 제공되는 단계;

<40> (i) 상기 (g)단계에서 상기 어플리케이션 모듈이 비인가된 것으로 확인될 경우, 해당 함수의 연산이 중지되는 단계;

<41> 가 포함되는데, 이때, 상기 함수가 쓰기를 요청하는 함수일 경우 상기 (e)단

계는,

<42> 상기 어플리케이션 모듈의 인가여부가 확인되는 단계;

<43> 상기 어플리케이션 모듈이 인가된 것으로 확인될 경우, 상기 함수의 연산이 중지되는 단계;

<44> 상기 어플리케이션 모듈이 비인가된 것으로 확인될 경우, 변경된 상기 함수가 연산이 가능하도록 복귀되어 상기 확장된 시스템 서비스 테이블로 제공되는 단계;

<45> 가 더 포함된다.

<46> 또한, 상기 암복호화모듈을 통해 상기 VSD이미지파일모듈과 VSD드라이브 간의 데이터 입출력이 암복호화 처리되는 단계;

<47> 가 더 포함된다.

<48> 이하 본 발명을 첨부된 예시도면에 의거하여 상세히 설명한다.

<49> 도 1은 본 발명에 따른 접근 통제시스템의 구동관계를 도시한 블럭도인바, 이를 참조하여 설명한다.

<50> 본 발명에 따른 접근 통제시스템은 내부 인가자에 의한 접속 시, 별도의 패스워드입력 또는 인증확인 절차와 같은 개별적인 확인과정없이 보안이 요구되는 데이터(이하 파일)에 대한 엑세스(여기서는 열기, 읽기, 쓰기 등의 작업수행을 위한 해당 파일에 대한 일련의 연산처리 ; 이하 접근)가 가능한 응용 프로그램(이하 어

플리케이션 모듈 ; A, A')을 선택적으로 인가하여 내부 인가자는 인가된 어플리케이션 모듈(A)을 통해서는 상기 파일에 대한 자유로운 열람 및 편집이 가능하도록 된다.

<51> 한편, 하드디스크(서버급에서는 DB로 명명되지만, 여기서는 일반 PC의 하드디스크와 더불어 DB까지 포괄하는 상위 개념으로 통칭)에 대한 물리적인 분할없이 가상디스크(VD)를 생성시켜 인가된 어플리케이션 모듈(A ; 인가된 응용프로그램)과 비인가된 어플리케이션 모듈(A' ; 비인가된 응용프로그램)에 대한 접근을 분리하였다. 상기 가상디스크(VD)에 대한 개념은 이하에서 보다 상세히 기술하겠다.

<52> 따라서, 도시된 바와 같이, 인가된 어플리케이션 모듈(A)은 보안이 요구되는 파일(이하 보안파일)만이 저장된 상기 가상디스크(VD)로 접근하여 읽기 및 쓰기(R/W ; Read/Write)를 실행할 수 있는 반면, 비인가된 어플리케이션 모듈(A')의 경우에는 가상디스크(VD)에 저장된 보안파일에 대한 읽기 및 쓰기 모두 불가능하고(X), 가상디스크(VD) 이외의 일반디스크(ND)에 저장된 파일에 대해서는 읽기 및 쓰기를 실행할 수 있게 된다.

<53> 한편, 인가된 어플리케이션 모듈(A)의 경우, 일반디스크(ND)에 저장된 파일에 대해 읽기는 가능하지만 쓰기는 실행할 수 없다. 이는 가상디스크(VD)에 저장되어 있는 보안파일이 외부로 유출되는 것을 막기 위함이며, 다음과 같은 실례를 통해 이해할 수 있다.

<54> 하나의 어플리케이션 모듈은 필요에 따라 다양한 확장자를 갖는 파일에 접근할 수 있도록 된다. 즉, "Adobe" 사의 "Photoshop 시리즈"나, "Acrobat Reader 시

리즈"와 같이 다양한 종류의 확장자를 갖는 그림파일을 열어보거나 편집할 수 있는 어플리케이션 모듈이 상기 가상디스크(VD)에 저장된 그림파일에 대한 접근이 가능하도록 인가된 어플리케이션 모듈(A)이라면, 상기 어플리케이션 모듈(A)을 통해 일반디스크(ND)에 저장된 비보안용 그림파일에 접근할 수도 있다. 이때, 일반디스크(ND)의 그림파일을 쓰기와 같은 편집을 한 후, 편집된 내용으로 갱신하여 저장할 수 있게 된다면 상기 가상디스크(VD)에 저장되어 있는 보안용 그림파일 또한 상기 인가된 어플리케이션 모듈(A)을 통해 상기 일반디스크(ND)로의 이동 또는 복사가 가능해 짐을 의미하게 된다. 따라서, 상기 가상디스크(VD) 내에 저장되어 있는 보안파일에 대한 무단유출을 원천적으로 막기 위해 본 발명에서는 인가된 어플리케이션 모듈(A)이 일반디스크(ND)에 저장된 파일로 접근하여 열어볼 수는 있어도 쓰기와 같은 편집은 할 수 없도록 되었다.

<55> 하지만, 상술된 기능은 본 발명에 따른 시스템의 적용사례에 따라 다르게 변형될 수도 있을 것이며, 필요에 따라 가상디스크(VD)에 접근하지 않은 상태에서는 보안파일을 일반디스크(ND)에 저장가능하도록 할 수도 있을 것이다.

<56> 상기한 기능을 수행하기 위해 본 발명은 다음과 같은 구성을 이루고 있으며, 본 발명에 따른 접근 통제시스템의 구성에 대한 일실시예를 도시한 도 2를 통해 이를 좀더 상세히 기술한다.

<57> 본 발명에 따른 접근 통제시스템은, 하드디스크(10)와, 디스크드라이브(20)와, 파일시스템 모듈(30)과, 어플리케이션 모듈(60)과, VSD이미지파일모듈(41)과, VSD드라이브(42)와, 암복호화모듈(45)과, VSD파일시스템 모듈(43)과, 접근통제장치

(44)가 포함된 구조를 갖는다.

<58> 상기 하드 디스크(10)는, 기본적으로 PC 또는 로컬 네트워크(LAN)가 구동되기 위해 필요한 데이터가 저장되며, 상기 데이터는 운영체제를 통해 파일형식으로 열람, 삭제 및 편집되어 관리된다. 해당 하드디스크(10)의 구체적인 물리적/화학적 구조 및 운영체제와의 작동관계에 있어서는 공지된 구성이므로 여기서는 이에 대한 상세한 설명은 피하기로 한다.

<59> 상기 디스크 드라이브(20)는, 상기 하드 디스크(20)를 관리하는 운영체제(OS)에 맞게 운용가능하도록 포맷된 디스크볼륨을 포함하며, 운영체제(OS)에서 이를 인식하여 연동된다. 일반적으로, 하드 디스크(10)에 대한 물리적인 디스크 분할 시, 각 분할된 영역별로 포맷된 디스크볼륨의 정보에 따라 디스크 드라이브가 지정되며, 운영체제(OS)는 이를 통해 하나의 하드 디스크(10)로부터 다수의 디스크 드라이브를 인식하여 관리하게 된다.

<60> 상기 디스크 드라이브(20) 또한 공지된 구성이므로 이에 대한 상세한 설명은 피하기로 한다.

<61> 상기 파일시스템 모듈(30)은, 상기 하드 디스크(10)의 물리적 특성을 추상화하여 논리적인 저장단위로 정리한 후 매핑된 파일로의 접근을 처리하는 것으로, 디스크볼륨에 대한 정보가 운영체제(OS)를 통해 인식되면, 운영체제(OS)와의 용이한 연동을 위해 설정된다. 즉, 컴퓨터에서 데이터를 기록하기 위해서는 상기 디스크 드라이브(20)에 데이터를 읽고, 쓰고, 찾기를 위한 준비를 해두어야 하는데, 파일시스템 모듈(30)은 그 준비의 규칙을 정리해 놓은 것이라 할 수 있으며, 파일에 이

름을 붙이거나, 데이터의 저장이나 검색을 위해 파일을 어디에 위치시킬 것인지를 나타내는 체계라 할 수 있다. 따라서, 하드 디스크(10)가 다수개의 디스크볼륨으로 분할되면, 이들을 각각 관리하는 파일시스템 모듈(30)이 운영체제(OS)를 통해 설정되어 이용자는 이들을 개별적으로 관리할 수 있게 된다.

<62> 참고로, 상기 파일시스템 모듈(30)에는 마이크로소프트사에서 개발된 컴퓨터 운영체제(OS)인 윈도우즈(WINDOWS)에서의 FAT16, FAT32, NTFS와, 리눅스의 ext2, raiserFS, ext3 등이 있으며, 본 발명에 따른 실시예에서는 상기 윈도우즈(WINDOWS)를 기본 운영체제(OS)로 하여 본 접근 통제시스템이 구현되므로, 파일시스템 모듈(30)로 FAT 시리즈, NTFS가 적용되었다. 하지만, 이는 일실시예에 불과하며, 이하의 청구범위를 벗어나지 않는 한도 내에서 다양하게 변형실시될 수 있다.

<63> 상기 어플리케이션 모듈(60)은, 운영체제(OS) 하에서 디스크볼륨에 저장된 파일을 불러와 구동시킬 수 있도록 된 일반적인 어플리케이션 모듈으로, 본 발명에서는 상기 가상디스크(VD)로의 접근여부를 인가받은 경우와 인가받지 못한 경우로 나뉘며, 이에 따라 본 발명의 구현도 다르게 이루어진다. 일반적으로, AutoCAD, Pro-E등의 CAD 프로그램등이 예가 될 수 있다.

<64> 어플리케이션 모듈(60)의 인가설정은, 각각의 응용 프로그램을 구분할 수 있는 정보(프로그램 이름, 헤더, Check sum, 또는 인증서)를 가져다 그 응용 프로그램인지 구분하고 룰을 정의해주는 것으로 되며, 상기 접근통제장치에서는 이 룰대로 동작하게 된다.

<65> 상기 VSD이미지파일 모듈(41)은, 상기 파일시스템 모듈(30)로 포맷된 디스크볼륨 내에 별도의 파일을 생성시킴으로서 이루어지며, 상기 디스크볼륨과 같이 하드 디스크(10) 상의 일정 공간을 파티션하여 상기 디스크볼륨 위에 또다른 가상 디스크볼륨을 형성시키는 것이다. 즉, 디스크분할과 같이 운영체제(OS)가 구현되기 전 하드 디스크의 물리적인 분할을 통해 각각의 디스크볼륨을 결정하고, 이에 대한 디스크드리이버를 지정한 후 운영체제(OS)에서 파일시스템 모듈을 설정하는 방식과는 달리, 운영체제(OS)를 통해 구현되어지고 있는 완전한 PC 및 로컬 네트워크(LAN) 상에서 사용자의 필요에 따라 하드 디스크를 분할한 것과 같은 효과를 얻을 수 있도록 된 것이다.

<66> 이때, 상기 VSD는 Virtual Secure Disk의 약자로, 여기서는 본 발명에서 보안파일을 저장하기 위해 형성시킨 가상디스크를 의미하며, 기존 하드디스크와의 구분 및 본 발명에 따라 더 구성된 요소들과의 차별화를 위해 사용되었다.

<67> 한편, 상기 VSD이미지파일 모듈에서의 '이미지'란, 실체하지는 않으면서 겉으로는 표현되어짐을 뜻하며, 여기서는 기존의 파일시스템모듈(30) 및 디스크드라이브(20)와 상기 가상디스크(VD)를 이루는 구성들간의 구분을 위해 사용될 것이다.

<68> 상기 VSD드라이브(42)는, 상기 VSD이미지파일 모듈(41)의 드라이브로써 상기 디스크 드라이브(20)에 대응되는 구성이다. 즉, VSD이미지파일 모듈(41)이 실질적으로는 일반파일(41')과 같은 파일의 개념으로 형성되었지만, 운영체제(OS) 상에서는 VSD이미지파일 모듈(41)이 별도로 디스크분할된 디스크볼륨으로 인식되어야 하므로 이에 저장된 파일들을 처리하는 VSD드라이브(42)가 요구된다 하겠다.

<69> 상기 VSD파일시스템 모듈(43)은, 상기 VSD이미지파일 모듈(41)과 VSD드라이브(42)의 생성으로 인해 운영체제(OS)에서는 새로운 디스크볼륨의 발생으로 인식되어 상기 VSD이미지파일모듈(41) 내 파일로의 접근을 처리하도록 설정되는 것이다.

<70> 따라서, VSD파일시스템 모듈(43)은 상기 파일시스템 모듈(30)에 대응되는 구성이다.

<71> 도 3은 본 발명에 따른 접근 통제시스템의 가상 디스크 설정과정을 도시한 블럭도인바 이를 참조하여 설명한다.

<72> 별도의 VSD설치프로그램(1)을 해당 PC 또는 로컬 네트워크(LAN) 상의 클라이언트 PC에 각각 인스톨하며, 상기 VSD설치프로그램(1)에 구성된 가상디스크볼륨생성수단(미도시됨)을 통해 상기 디스크볼륨 내 일정공간에 파일형식으로 공간을 점유하여 가상디스크볼륨을 생성시키고(2), VSD드라이브설정수단(미도시됨)을 통해 가상디스크볼륨에 해당하는 디바이스로 VSD드라이브(42)를 설정하는 한편, 상기 가상디스크볼륨에 대한 정보(DISK_GEOMETRY 정보, 파티션 정보 등)를 수신받는다.(3)

<73> 일반적으로, 상기 VSD설치프로그램(1) 인스톨 시, 가상디스크볼륨에 대한 정보를 결정된 상태이므로, 이에 따라 가상디스크볼륨이 생성되며, 상기 VSD드라이브(42)는 이에 대한 정보를 입력받게 될 것이다.

<74> 계속해서, VSD드라이브(42)가 설정되면, 운영체제(OS)에서는 해당 가상디스크볼륨에 대한 정보를 요청하게 되고(4), 이에 대응하여 VSD드라이브(42)에서는 앞서 수신된 가상디스크볼륨 정보를 생성한 후, 운영체제(OS)에 전달한다(5). 또한, 상기 운영체제(OS)는 당해 정보를 받아 이에 대한 범위에 상응하는 VSD파일시스템

모듈(43)을 설정하여 포맷하고, 새로운 디스크볼륨을 인식하게 된다.(6)

<75> 도 7a는 본 발명에 따른 접근 통제시스템의 인스톨 이전 상태를 보이는 '내 컴퓨터' 창이고, 도 7b는 본 발명에 따른 접근 통제시스템의 인스톨 이후 상태를 보이는 '내 컴퓨터' 창이다.

<76> 도면에서 보이는 바와 같이, 운영체제(OS)는 VSD이미지파일모듈(41)과 VSD드라이브(42)에 의해 디스크분할에 의한 또다른 하드디스크 드라이브가 생성된 것으로 인식하게 된다.

<77> 상기 암복호화모듈(45)은, 상기 VSD이미지파일모듈(41)과 VSD드라이브(42) 간의 데이터 입출력을 암복호화 처리하는 것으로서, 만약 VSD드라이브(42)에서 입출력 데이터를 그대로 VSD이미지파일모듈(41)에 저장한다면 VSD이미지파일모듈(41)을 해당 파일시스템모듈(30) 포멧으로 처리하여 그 속에 있는 보안파일들에 대한 정보가 모두 유출될 수 있기 때문에 VSD드라이브(42)가 VSD이미지파일모듈(41)에 입출력을 수행할 때는 암복호화를 수행해야 된다. 즉, 상기 보안파일은 상기 VSD이미지파일모듈(41) 내에 암호화되어 있지 않기 때문에 정보의 위치를 알 수만 없을 뿐이며 정보는 그대로 들어있어 완전한 보안을 이룰 수 없다.

<78> 예를 들어, VSD드라이브(42)에 VSD파일시스템모듈(43)의 WRITE 명령이 전달되면, WRITE할 데이터를 SECTOR 단위의 크기로 암호화를 수행한 후 VSD이미지파일모듈(41)에 기록하게 되고, READ 명령이 전달되면 VSD이미지파일모듈(41)에서 SECTOR 단위로 읽어서 복호화를 수행한 후 VSD파일시스템모듈(43)로 전달하게 된다.

<79> 이렇게 하면 VSD이미지파일모듈(41)이 유출된다 하더라도 파일의 내용이 암호화 되어 있으므로 VSD이미지파일모듈(41) 내의 보안파일이 공개될 수 없게 된다.

<80> 본 발명에서는 대칭키방식의 암복호화 방식을 채택하였으며, 대칭키방식에서도 특히 블록방식을 채용하였다. 이러한 블록방식은 디스크의 일섹터(512B) 단위로 블록화하여 암복호화가 수행되도록 된 것이다.

<81> 한편, 상기 보안파일(44)은 상기 VSD이미지파일모듈(41)에 저장되는 파일로, 보안이 요구되는 파일이라 하여 보안파일(44)로 명명된 것이다.

<82> 또한, 가상디스크라 함은 상기 VSD이미지파일모듈(41)과, VSD드라이브(42)를 아울러 명명된 것이다.

<83> 계속해서, 상기 접근통제장치(50)는, 상기 어플리케이션 모듈(60)에 의한 상기 디스크드라이브(20) 및 VSD드라이브(42) 내 저장파일로의 접근 시, 해당 작업이 진행되는 공간이 상기 디스크드라이브(20)인가 VSD드라이브(42)인가를 확인하고, 해당 파일로의 접근허가에 대한 어플리케이션 모듈(60)의 인가여부를 판별하여 접근을 결정하는 것이다.

<84> 일반적으로, 윈도우즈(WINDOWS ; 여기서는 NT 계열로 NT3.5, 4.0, 2000, XP 등이 있음)은 어플리케이션 모듈이 어떤 서비스를 요청 받았을 때 시스템 서비스 테이블(SST)을 통하여 서비스를 제공한다. 예를 들어, 어떤 어플리케이션 모듈이 파일을 오픈하거나 레지스트리 키를 오픈할 적에 그 어플리케이션 모듈은 CreateFile()이라는 Win32 API를 사용할 것이다. 이러한 API는 Kernel32.dll에 속해있는 가장 기본적인 함수로 구현되는데, 어플리케이션 모듈(A, A')로부터

CreateFile()(Kernel32.dll)이 호출되면, 운영체제(OS)는 NtCreateFile()(NTDLL.dll)을 거쳐 시스템 서비스 테이블(SST)로 ZwCreateFile()을 제공한다.

<85> 도 4a(종래 시스템 서비스 테이블의 구동관계를 도시한 블럭도)를 통해 보이는 바와같이, 어플리케이션 모듈(A, A')이 실행에 필요한 파일로의 접근을 위해 운영체제(OS)로 필요한 함수를 호출하면, 운영체제(OS)는 시스템 서비스 테이블(SST)에 해당 함수를 제공하여 디스크립터(D)를 통해 포인팅되도록 한다. 따라서, 어플리케이션 모듈(A, A')은 운영체제(OS) 하에 호환을 이루며 구현된다.

<86> 한편, 본 발명에 따른 접근 통제시스템은, 도 4b(본 발명에 따른 접근 통제 시스템에서 적용되는 시스템 서비스 테이블의 구동관계를 도시한 블럭도)에 도시된 바와 같이, 기존의 시스템 서비스 테이블(SST)이 확장된 시스템 서비스 테이블(NSST)로 대체되고, 이에 확장된 서비스 테이블(NST)이 더 포함되면서 도 5(도 4b의 구성에 따라 응용 프로그램(어플리케이션 모듈)에 의한 해당 파일의 접근 허가 여부가 진행되는 플로우를 도시한 예제)에 도시된 바에 따른 과정이 수행된다.

<87> 어플리케이션 모듈(A, A')이 실행에 필요한 파일로의 접근을 위해 운영체제(OS)로 필요한 함수를 호출하면, 운영체제(OS)는 해당 함수를 상기 확장된 서비스 테이블(NST)로 제공하여 다음과 같은 연산이 수행되도록 한다.

<88> 우선 어플리케이션 모듈(A, A')에서, CreateFile()에 대한 함수를 호출하면, 운영체제(OS)는 NtCreateFile()(ntdll.dll)을 거쳐 확장된 서비스 테이블(NST)로 ZwCreateFile()을 제공한다. 이때, 상기 확장된 서비스 테이블(NST)은

ZwCreateFile()을 OnZwCreateFile()(해당 함수가 진행되지 못하도록 본 발명에서 임의로 설정한 함수)로 일단 변경한 후, 논리를 통해 상기 확장된 시스템 서비스 테이블(NSST)에서의 해당 함수에 대한 연산여부를 결정짓게 된다.

<89> 이때, 본 발명에 따른 실시예에서, 상기 OnZwCreateFile() 함수는 어플리케이션 모듈(A, A')이 해당 함수인 CreateFile()을 요청할 경우 상기 확장된 시스템 서비스 테이블(NSST)에 ZwCreateFile()가 곧바로 제공되면서 디스크립터(D)가 포인팅하지 못하도록, 해당 함수인 CreateFile()을 요청할 경우 다음 진행이 상기 확장된 서비스 테이블(NST)의 OnZwCreateFile()로 되도록 번지를 변경한 후, 상기 논리가 진행되도록 하여 상기 논리가 완성되기 전에는 디스크립터(D)에 의한 포인팅이 이루어지지 못하도록 하였다. 여기서 상기 임의로 생성된 OnZwCreateFile()라 함은 본 발명에서 상기 확장된 서비스 테이블(NST)이 더 설치되면서 종래 시스템 서비스 테이블(SST)에 있던 함수가 이미 변경/대체된 것이다.

<90> 한편, 상기 논리는 호출되는 상기 함수의 목적이 되는 파일의 위치가 가상디스크(VD)인가 일반디스크(ND)인가에 대한 확인과, 상기 함수를 호출하는 어플리케이션 모듈(A, A')의 인가여부 확인으로써, 예제를 통해 보인 바와 같이, 가상디스크(VD)로 확인되면, 인가된 어플리케이션 모듈(A)인가를 확인하여 인가된 것일 경우, 상기 확장된 시스템 서비스 테이블(NSST)로 변경 이전의 함수인 ZwCreateFile()를 제공하고, 그렇지 않을 경우에는 해당 함수의 연산을 중지한다.(False) 또한, 앞 단계에서 일반디스크(ND)로 확인되면, 어플리케이션 모듈(A, A')의 인가여부 확인은 생략하고 상기 확장된 시스템 서비스 테이블(NSST)로 변경

이전의 함수인 ZwCreateFile()를 제공한다.

<91> 한편, 상기 디스크립터(D)는 상기 시스템 서비스 테이블(SST)이 아닌, 상기 확장된 시스템 서비스 테이블(NSST)로 포인팅 된다.

<92> 도 4b에서 시스템 서비스 테이블(SST)과 확장된 시스템 서비스 테이블(NSST)을 연결하고 있는 파선의 화살표는 상기 파일접근에 실질적으로 관여되는 상기 함수들 이외에 어플리케이션 모듈(A, A')의 구현에 필요한 다른 종류의 함수호출 시, 상기 확장된 서비스 테이블(NST)에서의 논리과정없이 해당 함수를 상기 확장된 시스템 서비스 테이블(NSST)에 곧바로 제공하여 함수의 연산을 진행시킬 수 있다.

<93> 이상, 상기 접근통제장치(50)는 상술된 과정을 통해 가상디스크(VD) 내에 존재하는 파일에 대한 보안기능을 수행하게 된다.

<94> 한편, 상술된 바와 같이, 함수에 의한 보안파일로의 접근이 인가된 어플리케이션 모듈(A) 이외에는 허용되지 않으므로, 본 발명에 따른 가상디스크(VD)는 비인가된 어플리케이션 모듈(A')에 의한 접근시도 시, 도 7a에서와 같이 드라이브 자체가 확인이 되지 않아 애초부터 불가할 뿐만아니라, 도 8(본 발명에 따른 접근 통제 시스템의 가상 디스크가 파일로 인식되어지는 모습을 보이는 창)에서와 같이 상기 VSD이미지파일모듈(41)은 열 수 없는 파일형식으로 존재되어 비인가된 어플리케이션 모듈(A')으로는 그 접근이 불가능하게 된다.

<95> 도 9는 허가되지 않은 어플리케이션을 통한 가상 디스크로의 접근시 그 시도가 거부됨을 보이는 창으로, 비인가된 어플리케이션 모듈(A') 또는 운영체제(OS) 상에서 파일형식으로 존재하는 상기 VSD이미지파일모듈(41)에 대한 열기를 시도할

경우, 접근이 거부되고 있음을 보이고 있다.

<96> 이상, 본 발명에 따른 접근 통제시스템의 구성을 보았으며, 이하에서는 이를 통한 통제 방법에 대해 설명한다.

<97> 이하에서 기재되는 함수인 ReadFile() 및 WriteFile()은, 상기 CreateFile() 함수가 읽기모드 또는 쓰기모드로 전환/실행될 때 호출되는 함수로서, 본 발명에 따른 접근 통제시스템 하에서 보안파일에 대한 읽기 및 쓰기의 통제방법이 각각 명확히 구분되도록 각 모드별로 해당 함수를 구분하여 기술하였다.

<98> 참고로, 어플리케이션 모듈을 통해 임의의 파일로 접근하기 위해서는 파일 핸들러인 CreateFile()을 우선적으로 호출하게 되며, CreateFile() 호출에 의해 제공되는 ZwCreateFile()가 상기 ReadFile() 또는 WriteFile()를 각각 호출하면서 읽기모드 또는 쓰기모드로 실행되고, 이로인해 어플리케이션 모듈에서 해당 파일의 읽기 또는 쓰기가 진행된다.

<99> 상기 어플리케이션 모듈을 선택적으로 인가하는 단계(1);

<100> 가상디스크(VD)에 접근할 수 있는 어플리케이션 모듈(60)을 지정하여 인가하는 단계이다. 어플리케이션 모듈(60)의 인가방식에 대한 실시예는 상술된 바 있으므로 여기서는 그 설명을 생략하기로 한다.

<101> 상기 어플리케이션 모듈(60)이 해당 파일로의 접근을 위해 함수를 호출하는 단계(2);

<102> 도 6a(본 발명에 따른 접근 통제시스템에서 응용 프로그램을 통한 해당 파일의 읽기과정을 도시한 플로우차트)에서, 시작(어플리케이션 모듈의 디스크 읽기 시도) 부분에 해당하는 것으로, 어플리케이션 모듈(60)이 구현에 필요한 파일의 읽기를 요청하고 이를 위해 ReadFile() 함수를 호출하는 단계이다.

<103> 상기 함수를 변경하여 대기상태로 하는 단계(3);

<104> 상기 단계(2)가 진행되면, 상기 접근통제장치(50)에 포함된 확장된 서비스 테이블(NST)로 상기 함수가 제공되되, 확장된 서비스 테이블(NST)은 상기 ReadFile()함수를 OnZwReadFile()로 변경하여 어플리케이션 모듈(60)의 실행에 요구되는 논리를 진행한다.

<105> 상기 파일로의 접근공간이 상기 디스크드라이브인지 VSD드라이브인지를 확인하는 단계(4);

<106> 여기서는 가상디스크인지 여부를 확인하는 과정으로, 도 6a 상의 (S1)에 해당된다.

<107> 상기 단계(4)에서 디스크드라이브로 확인될 경우, 연산이 불가능하도록 변경된 함수를 원래의 함수로 복귀시켜 제공하는 단계(5);

<108> 상기 파일이 위치하는 공간이 디스크드라이브(20)로 확인되면, 상기 확장된 서비스 테이블(NST)은 OnZwReadFile() 함수의 변경 전 함수인 ZwReadFile()를 상기 확장된 시스템 서비스 테이블(NSST)로 제공하여 해당 함수의 연산을 속행하게 되고, 이로인해 해당 파일에 대한 읽기를 허용한다.(S4)

<109> 상기 단계(4)에서 VSD드라이브로 확인될 경우, 상기 어플리케이션 모듈의 접

근이 인가된 것인가를 확인하는 단계(6);

<110> 반면, VSD드라이브(42)로 확인되면, 그 다음 논리로서 상기 어플리케이션 모듈(60)이 인가된 어플리케이션 모듈인지 여부를 확인한다.(S2)

<111> 상기 단계(6)에서 인가된 것으로 확인될 경우, 연산이 불가능하도록 변경된 함수를 원래의 함수로 복귀시켜 제공하는 단계(7);

<112> 상기 어플리케이션 모듈(60)이 인가된 어플리케이션 모듈으로 확인되면, 상기 확장된 서비스 테이블(NST)은 OnZwReadFile() 함수의 변경 전 함수인 ZwReadFile()를 상기 확장된 시스템 서비스 테이블(NSST)로 제공하여 해당 함수의 연산을 속행하게 되고, 이로인해 해당 파일에 대한 읽기를 허용한다.(S4)

<113> 상기 단계(6)에서 비인가된 것으로 확인될 경우, 해당 함수의 연산을 중지하는 단계(8);

<114> 반면, 어플리케이션 모듈이 비인가된 것으로 확인되면, 상기 확장된 시스템 서비스 테이블(NSST)에서의 해당함수에 대한 연산이 중지되어 읽기가 불허된다.(S3)

<115> 계속해서, 상기 함수가 WriteFile()일 경우에는 상기 단계(5)의 과정에 있어서, 이하의 단계가 더 포함된다. 이는 도 6b(본 발명에 따른 접근 통제시스템에서 응용 프로그램을 통한 해당 파일의 쓰기과정을 도시한 플로우차트)와 더불어 설명한다. 이때, 상기 함수인 WriteFile()는 확장된 서비스 테이블(NST)에서 OnZwWriteFile() 변경된다.

<116> 상기 어플리케이션 모듈의 인가여부를 확인하는 단계(5-1);

<117> 디스크드라이브(20)로 확인된 상태에서, 해당 함수를 호출하는 어플리케이션 모듈(60)이 인가된 어플리케이션 모듈인지 여부를 확인한다.(S30)

<118> 상기 단계(5-1)에서 인가된 것으로 확인될 경우, 해당 함수의 연산을 중지하는 단계(5-2);

<119> 상기 단계(5-1)에서 인가된 어플리케이션 모듈으로 확인되면, 상기 확장된 서비스 테이블(NST)은 확장된 시스템 서비스 테이블(NSST)에서의 해당 함수에 대한 연산이 중지되어 쓰기가 불허된다.(S31)

<120> 상기 단계(5-2)에서 비인가된 것으로 확인될 경우, 연산이 불가능하도록 변경된 함수를 원래의 함수로 복귀시켜 제공하는 단계(5-3);

<121> 상기 단계(5-1)에서 비인가된 어플리케이션 모듈으로 확인되면, 상기 확장된 서비스 테이블(NST)은 OnZwWriteFile()의 변경 전 함수인 ZwWriteFile()로 복귀시켜 상기 확장된 시스템 서비스 테이블(NSST)로 제공하고, 이를 디스크립터(D)가 포인팅함으로서, 해당 함수의 연산을 통한 쓰기가 허용된다.(S40)

<122> 읽기 함수에 대한 통제 방법에 쓰기 함수에 대한 통제 방법의 상기 단계가 더 포함되어야 하는 이유는 상술한 바 있으므로 여기서는 생략하기로 한다.

<123> 한편, 상술한 바와 같이, 상기 VSD이미지파일모듈(41)은 기존 디스크볼륨에 파일형식으로 위치되고 있으므로, VSD이미지파일모듈(41) 만을 카피하거나 잘라내기를 한 후 기존의 파일시스템모듈(30)을 통해 접근하여 유출시킬 수도 있으므로, 상기 암복호화모듈(45)을 통해 상기 VSD이미지파일모듈(41)과 VSD드라이브(42) 간의 데이터 입출력을 암복호화 하는 단계가 더 포함되어야 한다.

【발명의 효과】

<124> 이상 상기와 같은 본 발명에 따르면, 기존의 하드디스크를 물리적으로 분할할 필요없이 현재 운영체제에 의해 운영되는 시스템 내에 별도의 가상디스크를 생성시켜 별도의 파일시스템을 통해 새로운 드라이브로써 관리되는 한편, 이 드라이브에 저장된 보안파일로의 접근 시 인가된 응용프로그램(어플리케이션 모듈)에 대해서만 허용되므로, 내부 인가자에 대한 개별적인 확인절차 없이도 상기 응용프로그램(어플리케이션 모듈)이 설치된 PC라면 번거로운 절차없이도 보안파일로의 접근을 이룰 수 있는 반면, 인가된 응용프로그램(어플리케이션 모듈) 상에서만이 보안파일에 대한 접근이 가능하므로, 보안파일를 복사하거나 잘라내기를 통해 외부로 유출시킬 수도 없으며, 외부로부터 침입되는 불법적인 접근은 애초부터 불가능하게 된다.

<125> 또한, 보안파일에 각각 암호화 또는 사용권한 부여작업을 하지 않아도 상기 가상디스크 상에 별도로 저장되어 보호되므로, 파일보안에 필요한 작업이 보다 용이해지는 효과가 있다.

【특허청구범위】

【청구항 1】

하드디스크의 일정공간을 파일형식으로 점유하는 VSD이미지파일모듈과;

상기 VSD이미지파일모듈 내의 보안파일을 처리하는 VSD드라이브와;

상기 VSD이미지파일모듈과 VSD드라이브 간의 데이터 입출력을 암복호화 처리하는 암복호화모듈과;

상기 VSD드라이브를 통해 운영체제가 별도의 디스크볼륨이 생성된 것으로 인식시켜 상기 VSD이미지파일모듈 내 보안파일로의 접근을 처리하는 VSD파일시스템모듈과;

상기 어플리케이션 모듈에 의한 상기 디스크드라이브 및 VSD드라이브 내 파일로의 접근 시, 해당 작업이 진행되는 공간이 상기 디스크드라이브인가 VSD드라이브인가를 확인하고, 해당 파일로의 접근허가에 대한 어플리케이션 모듈의 인가여부를 판별하여 접근을 결정하는 접근통제장치;

가 포함된 것을 특징으로 하는 접근 통제시스템.

【청구항 2】

제 1 항에 있어서, 상기 접근통제장치는

디스크립터에 의해 포인팅되어 해당 함수의 연산이 진행되도록 하는 확장된 시스템 서비스 테이블과; 상기 어플리케이션 모듈이 상기 시스템 서비스 테이블에 요청한 함수를 연산되지 못하도록 변경한 후, 해당 작업이 진행되는 공간이 상기

디스크드라이브인가 VSD드라이브인가를 확인하고 해당 파일로의 접근허가에 대한 어플리케이션 모듈의 인가여부를 판별하여, 그 결과에 따라 상기 확장된 시스템 서비스 테이블로 변경이전의 상기 함수를 제공하거나 그 함수의 연산중지를 선택적으로 결정하는 확장된 서비스 테이블이 포함된 것을 특징으로 하는 접근 통제시스템.

【청구항 3】

하드디스크와, 디스크드라이브와, 파일시스템 모듈과, 어플리케이션 모듈과, VSD이미지파일모듈과, VSD드라이브와, 암복호화모듈과, VSD파일시스템 모듈과, 확장된 시스템 서비스 테이블과 확장된 서비스 테이블을 포함하는 접근통제장치로 된 접근 통제시스템을 통하여,

(a) 상기 어플리케이션 모듈이 선택적으로 인가되는 단계;

(b) 상기 어플리케이션 모듈에 의한 해당 파일로의 접근을 위해 운영체제로 함수가 호출되는 단계;

(c) 상기 운영체제에 의해 상기 함수가 상기 확장된 서비스 테이블로 제공되는 단계;

(d) 상기 확장된 서비스 테이블에서 상기 함수의 연산이 중지되도록 임의로 지정된 함수로 변경되는 단계;

(e) 상기 확장된 서비스 테이블에서 어플리케이션 모듈에 의한 상기 파일로의 접근공간이 상기 디스크드라이브인지 VSD드라이브인지가 확인되는 단계;

(f) 상기 (e)단계에서 디스크드라이브로 확인될 경우, 변경된 상기 함수가

연산이 가능하도록 복귀되어 상기 확장된 시스템 서비스 테이블로 제공되는 단계;

(g) 상기 (e)단계에서 VSD드라이브로 확인될 경우, 상기 어플리케이션 모듈의 접근이 인가된 것인가가 확인되는 단계;

(h) 상기 (g)단계에서 상기 어플리케이션 모듈이 인가된 것으로 확인될 경우, 변경된 상기 함수가 연산이 가능하도록 복귀되어 상기 확장된 시스템 서비스 테이블로 제공되는 단계;

(i) 상기 (g)단계에서 상기 어플리케이션 모듈이 비인가된 것으로 확인될 경우, 해당 함수의 연산이 중지되는 단계;

가 포함된 것을 특징으로 하는 가상 디스크를 이용한 응용 프로그램 별 접근 통제방법.

【청구항 4】

제 3 항에 있어서, 상기 함수가 쓰기를 요청하는 함수일 경우 상기 (e)단계는,

상기 어플리케이션 모듈의 인가여부가 확인되는 단계;

상기 어플리케이션 모듈이 인가된 것으로 확인될 경우, 상기 함수의 연산이 중지되는 단계;

상기 어플리케이션 모듈이 비인가된 것으로 확인될 경우, 변경된 상기 함수가 연산이 가능하도록 복귀되어 상기 확장된 시스템 서비스 테이블로 제공되는 단계;

가 더 포함된 것을 특징으로 하는 가상 디스크를 이용한 응용 프로그램 별 접근 통제방법.

【청구항 5】

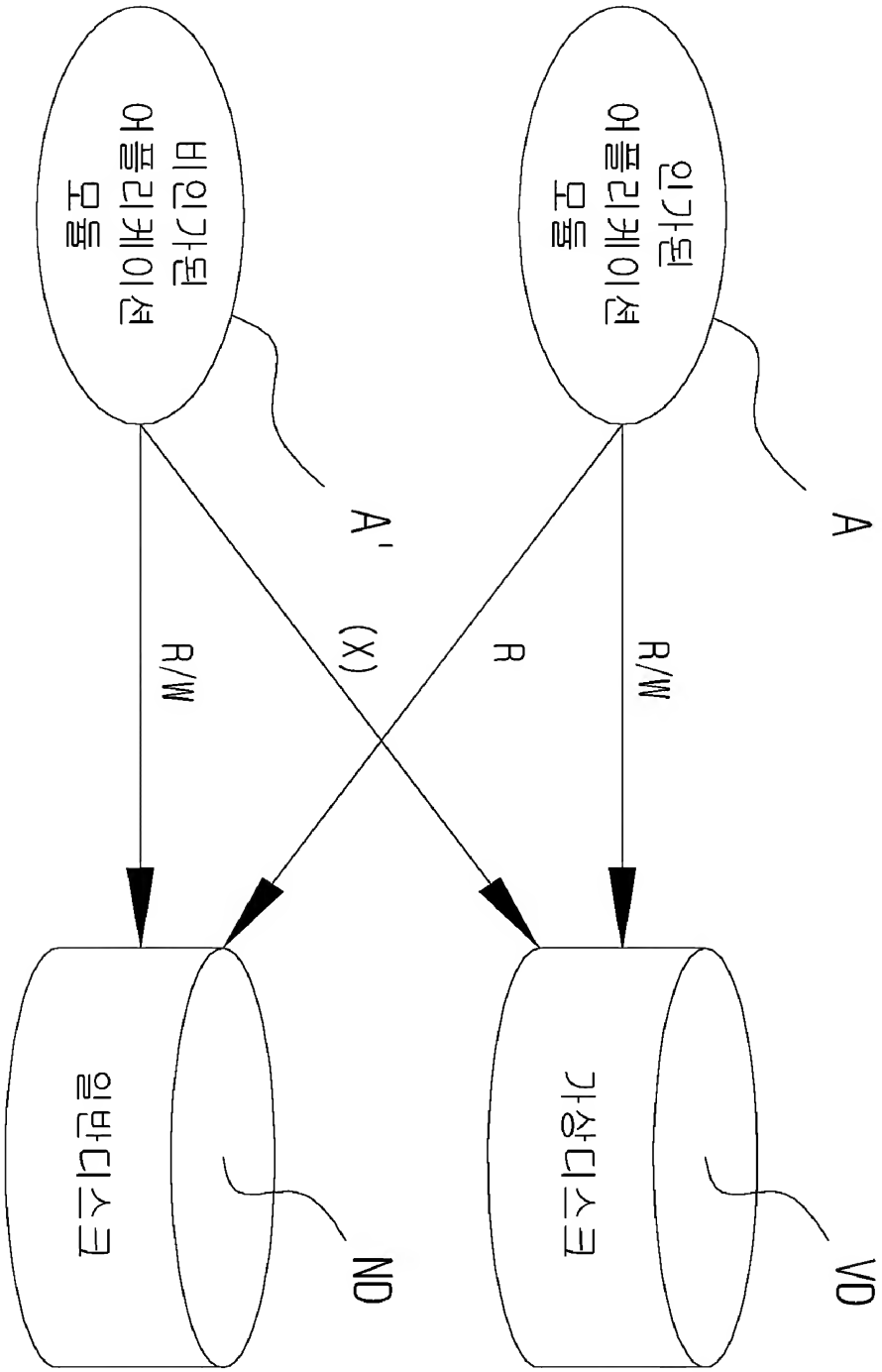
제 3 항 또는 제 4 항에 있어서,

상기 암복호화모듈을 통해 상기 VSD이미지파일모듈과 VSD드라이브 간의 데이터 입출력이 암복호화 처리되는 단계;

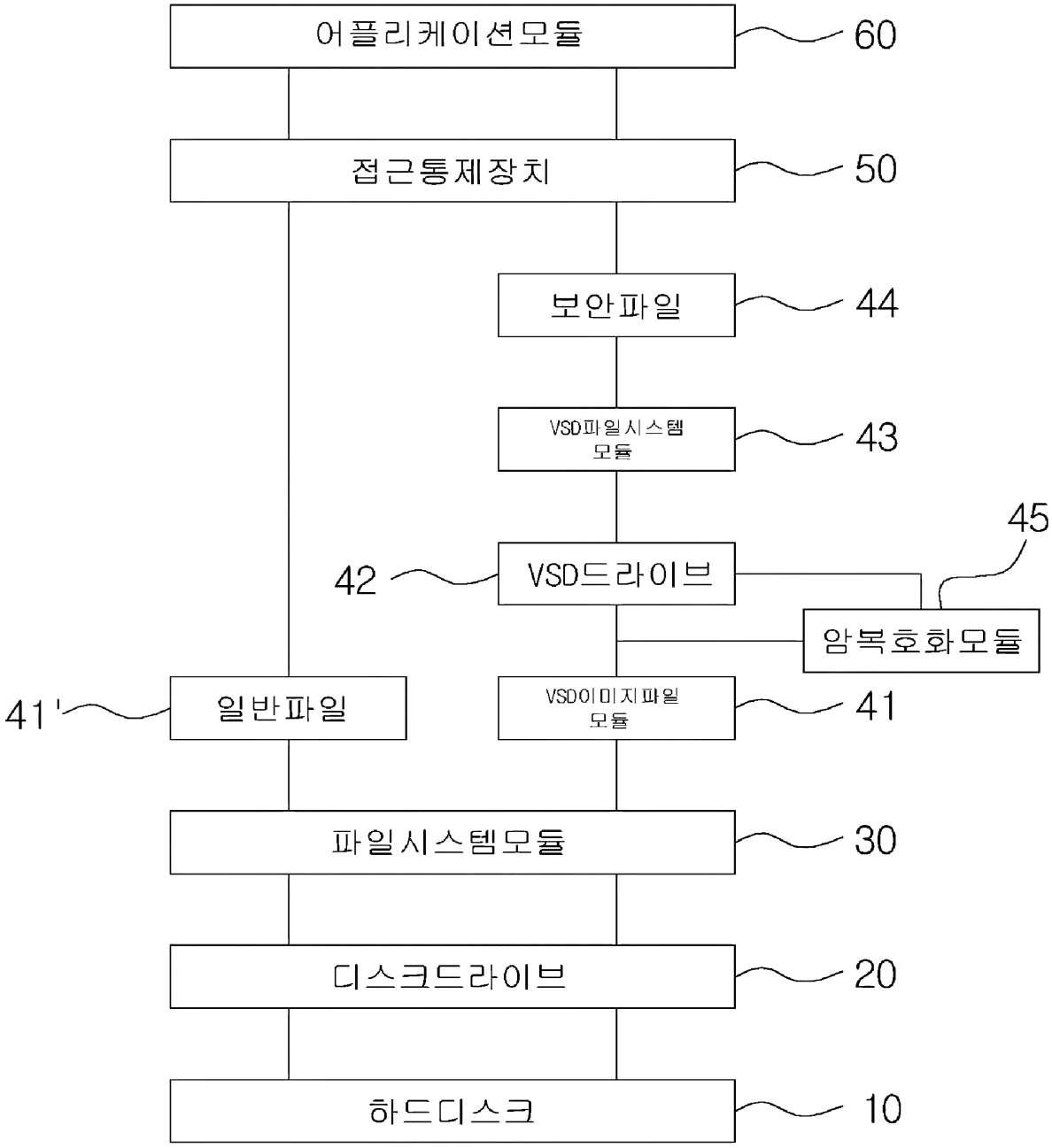
가 더 포함된 것을 특징으로 하는 가상 디스크를 이용한 응용 프로그램 별 접근 통제방법.

【도면】

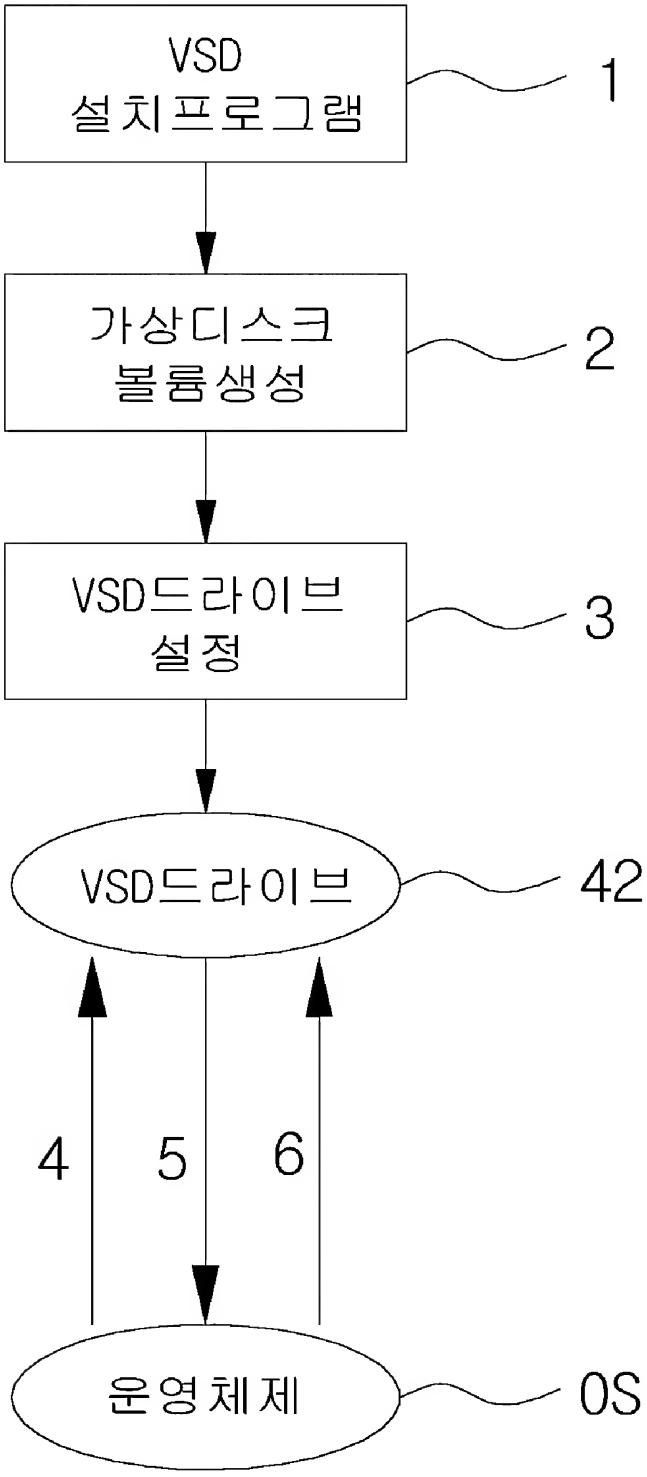
【도 1】



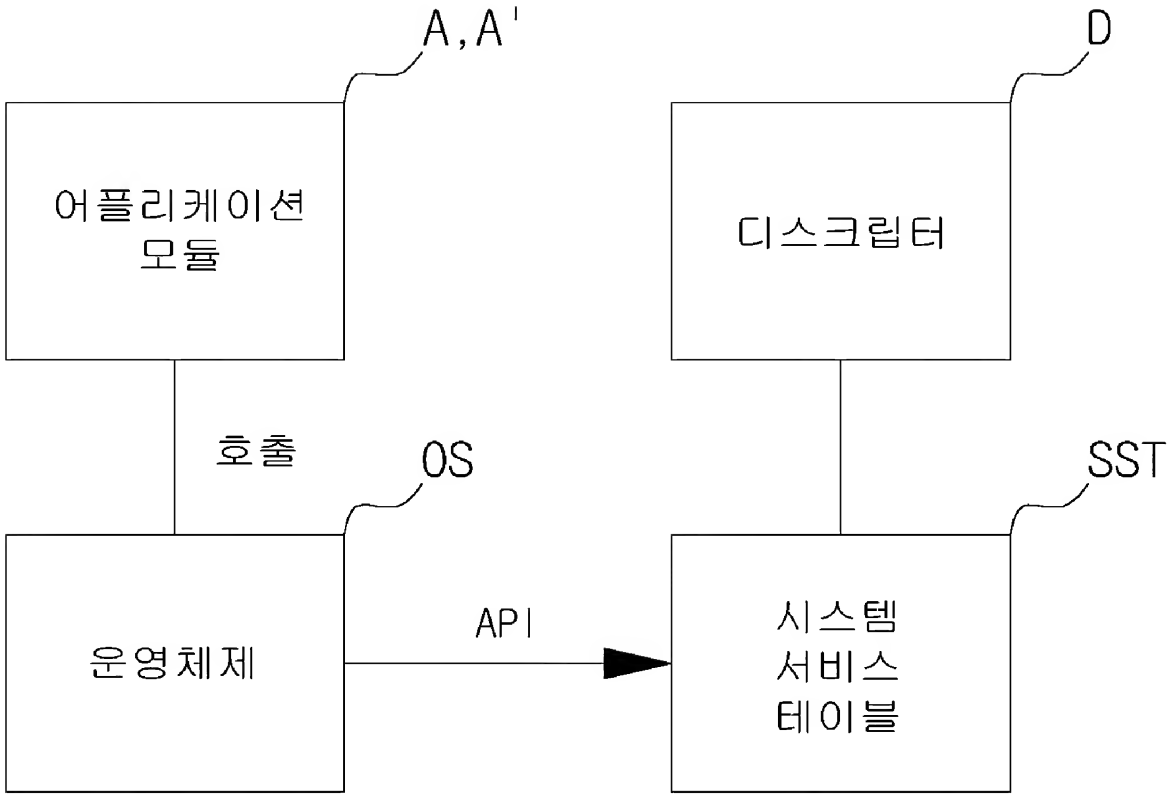
【도 2】


어플리케이션모듈
60
접근통제장치
50
보안파일
44
VSD파일시스템
모듈
43
45
42
VSD드라이브
암복호화모듈
41'
일반파일
VSD이미지파일
모듈
41
파일시스템모듈
30
디스크드라이브
20
하드디스크
10

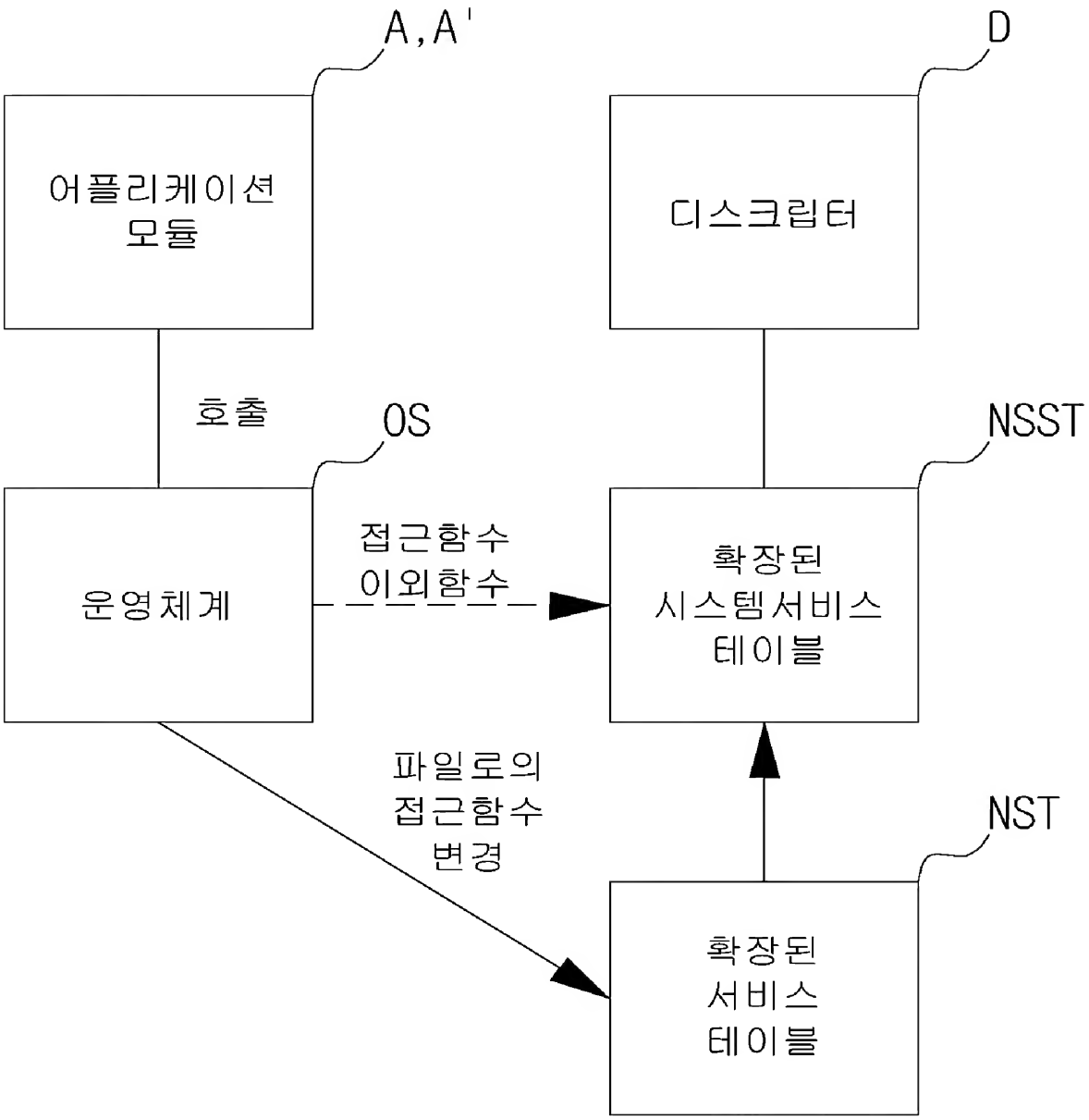
【도 3】



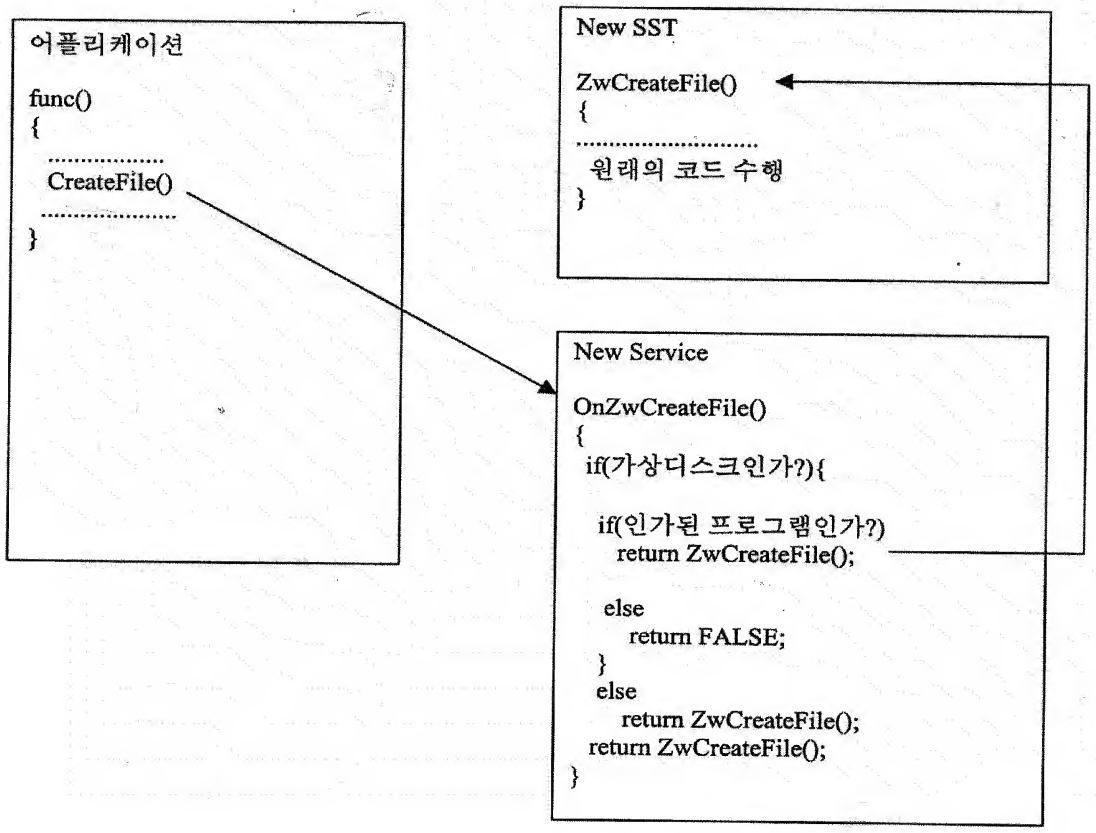
【도 4a】



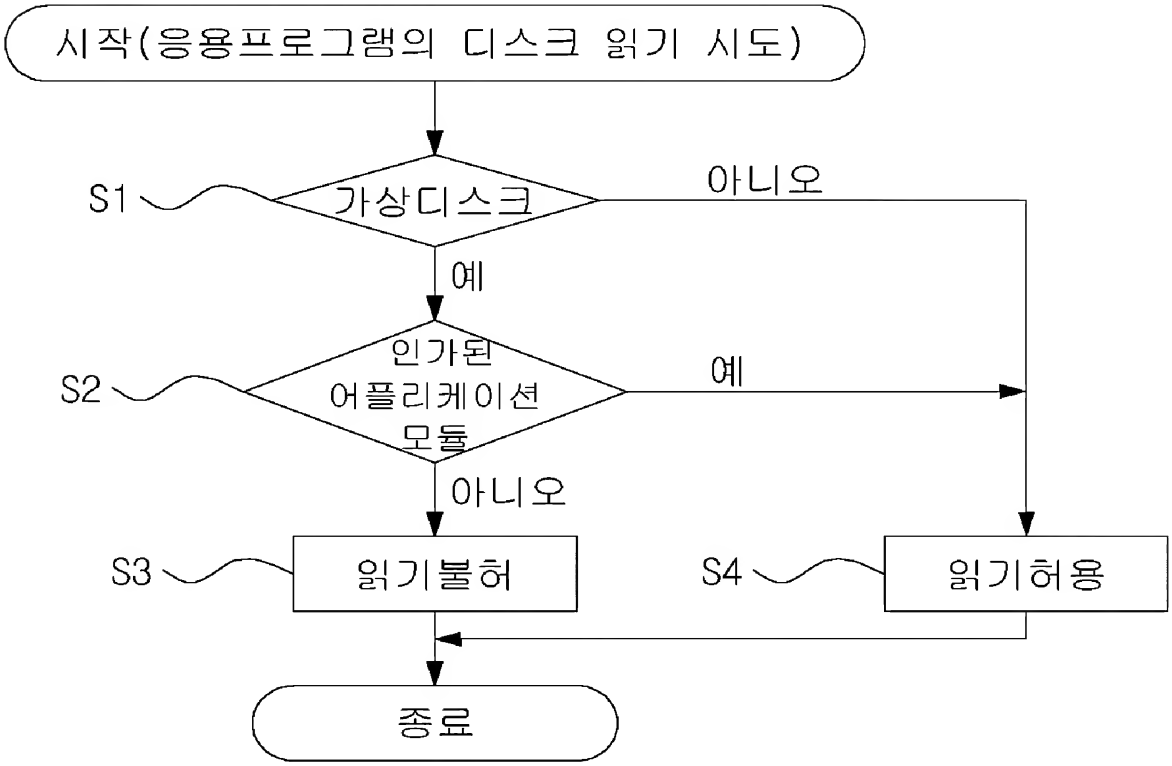
【도 4b】


A,A'
D
어플리케이션
모듈
디스크립터
호출
OS
NSST
접근함수
이외함수
운영체계
확장된
시스템서비스
테이블
파일로의
접근함수
변경
NST
확장된
서비스
테이블

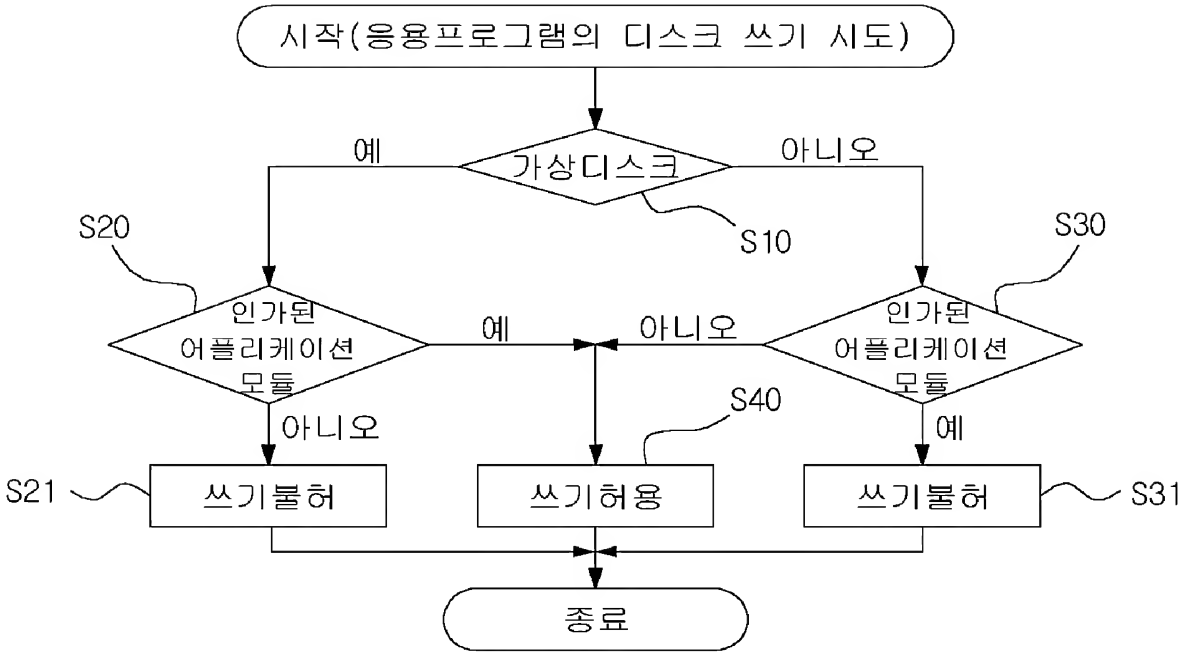
【도 5】


어플리케이션
func()
{
CreateFile()
}
New SST
ZwCreateFile()
{
원래의 코드 수행
}
New Service
OnZwCreateFile()
{
if(가상디스크인가?){
if(인가된 프로그램인가?)
return ZwCreateFile();
else
return FALSE;
}
else
return ZwCreateFile();
return ZwCreateFile();
}

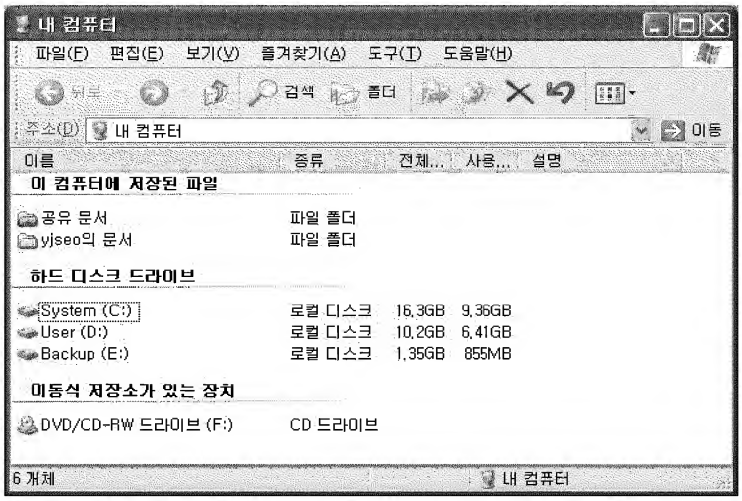
【도 6a】


시작(응용프로그램의 디스크 읽기 시도)
S1
가상디스크
아니오
예
S2
인가된
어플리케이션
모듈
예
아니오
S3
읽기불허
S4
읽기허용
종료

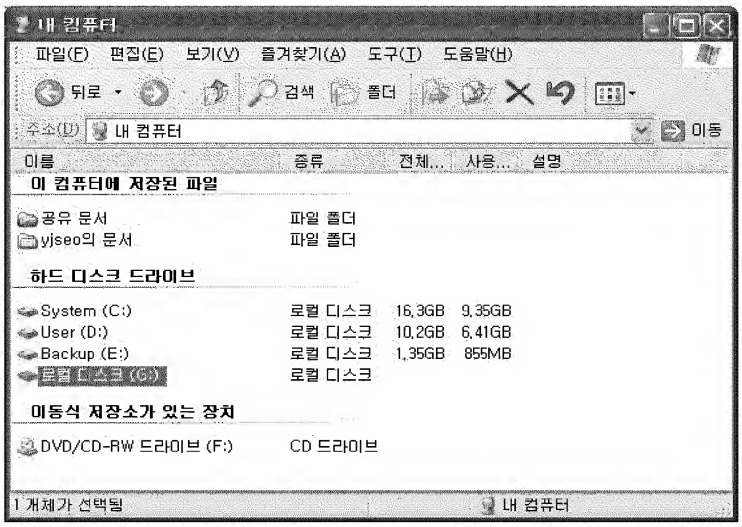
【도 6b】


시작(응용프로그램의 디스크 쓰기 시도)
가상디스크
예
아니오
S10
S20
S30
인가된 어플리케이션 모듈
예
아니오
인가된 어플리케이션 모듈
아니오
예
S40
S21
쓰기불허
쓰기허용
쓰기불허
S31
종료

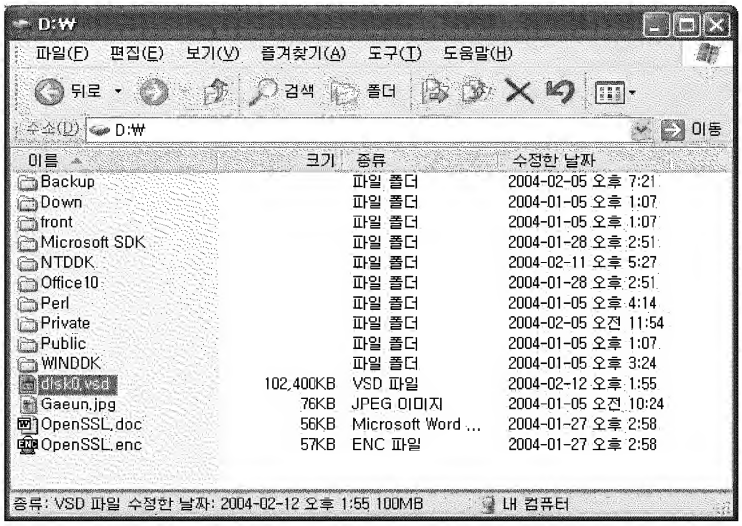
【도 7a】


내 컴퓨터
파일(F) 편집(E) 보기(V) 즐겨찾기(A) 도구(T) 도움말(H)
뒤로 검색 폴더
주소(D) 내 컴퓨터
이동
이름 종류 전체... 사용... 설명
이 컴퓨터에 저장된 파일
공유 문서 파일 폴더
yjseo의 문서 파일 폴더
하드 디스크 드라이브
System (C:) 로컬 디스크 16.3GB 9.36GB
User (D:) 로컬 디스크 10.2GB 6.41GB
Backup (E:) 로컬 디스크 1.35GB 855MB
이동식 저장소가 있는 장치
DVD/CD-RW 드라이브 (F:) CD 드라이브
6 개체
내 컴퓨터

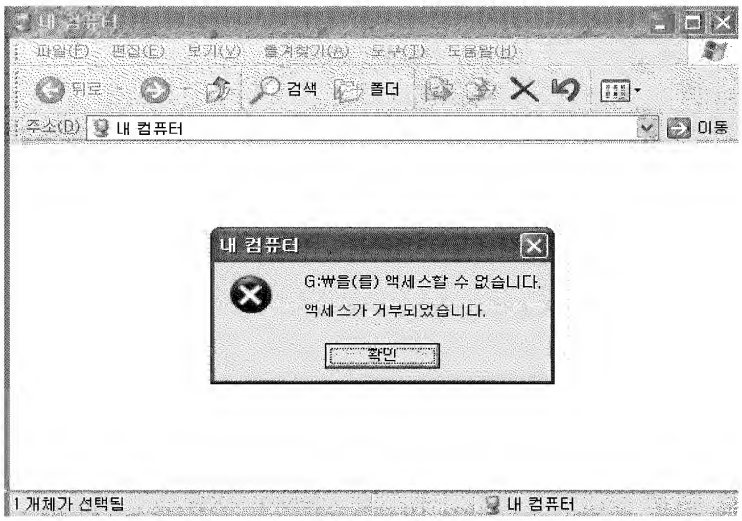
【도 7b】


내 컴퓨터
파일(F) 편집(E) 보기(V) 즐겨찾기(A) 도구(T) 도움말(H)
뒤로 검색 폴더
주소(D) 내 컴퓨터
이동
이름 종류 전체... 사용... 설명
이 컴퓨터에 저장된 파일
공유 문서 파일 폴더
yjseo의 문서 파일 폴더
하드 디스크 드라이브
System (C:) 로컬 디스크 16.3GB 9.35GB
User (D:) 로컬 디스크 10.2GB 6.41GB
Backup (E:) 로컬 디스크 1.35GB 855MB
로컬 디스크 (G:) 로컬 디스크
이동식 저장소가 있는 장치
DVD/CD-RW 드라이브 (F:) CD 드라이브
1 개체가 선택됨
내 컴퓨터

【도 8】


D:₩
파일(F) 편집(E) 보기(V) 즐겨찾기(A) 도구(T) 도움말(H)
뒤로 검색 폴더
주소(D) D:₩
이동
이름 크기 종류 수정한 날짜
Backup 파일 폴더 2004-02-05 오후 7:21
Down 파일 폴더 2004-01-05 오후 1:07
front 파일 폴더 2004-01-05 오후 1:07
Microsoft SDK 파일 폴더 2004-01-28 오후 2:51
NTDDK 파일 폴더 2004-02-11 오후 5:27
Office10 파일 폴더 2004-01-28 오후 2:51
Perl 파일 폴더 2004-01-05 오후 4:14
Private 파일 폴더 2004-02-05 오전 11:54
Public 파일 폴더 2004-01-05 오후 1:07
WINDDK 파일 폴더 2004-01-05 오후 3:24
disk0.vsd 102,400KB VSD 파일 2004-02-12 오후 1:55
Gaeun.jpg 76KB JPEG 이미지 2004-01-05 오전 10:24
OpenSSL.doc 56KB Microsoft Word ... 2004-01-27 오후 2:58
OpenSSL.enc 57KB ENC 파일 2004-01-27 오후 2:58
종류: VSD 파일 수정한 날짜: 2004-02-12 오후 1:55 100MB
내 컴퓨터

【도 9】


내 컴퓨터
파일(F) 편집(E) 보기(V) 즐겨찾기(A) 도구(T) 도움말(H)
뒤로
검색
폴더
주소(D) 내 컴퓨터
이동
내 컴퓨터
G:₩을(를) 액세스할 수 없습니다.
액세스가 거부되었습니다.
확인
1 개체가 선택됨
내 컴퓨터